那覇市教育委員会EDR導入及び運用・保守事業仕様書

那覇市教育委員会　教育研究所

1.件名

那覇市教育委員会EDR導入及び運用・保守事業

2.利用期間

想定期間：令和6年8月1日～令和11年7月31日

3.本業務の目的

近年、サイバー攻撃や不正アクセスなどのセキュリティ犯罪が急増している。

教育機関においては、教師や児童・生徒の個人情報や学校の業務データが扱われることから、セキュリティ対策がますます重要視されている。また、文部科学省が令和５年３月に公開した「GIGAスクール構想の下での校務DXについて」（P15～P18参照）によれば、教育現場での高度な情報セキュリティ対策の実施が求められている。

そこで、那覇市教育委員会では、セキュリティ強化のため教育ネットワークに接続されるクライアント端末へのEDR（Endpoint Detection and Response）*1の導入を行うこととする。

*1 クライアント端末における不信な挙動を検知し、迅速な対応を支援するセキュリティソリューション

4.本業務の基本的な考え方

4.1.システム構築手法

本システムの構築にあたっては、パッケージソフトを活用することを基本とし、必要に応じてカスタマイズ

(アドオンを含む。)を加えることで本仕様の要求事項を満たすものとする。

4.2.操作環境

本システムはシステムを管理するサーバーと管理画面、クライアント端末側ソフト（以降エージェントと言う）からなるものとし、下記の要件をみたすものとする。

※管理するクライアント端末にはマイクロソフトWindows10以降のOSが搭載されているものとする。

※将来的な拡張を鑑みて、Windows Server、MacOS、主要なLinuxディストリビューションにもインストールできること。

・管理画面はWebベースで稼働するものとし、ウェブ標準に対応したブラウザ（グーグルChrome、マイクロソフトEdge含む）のバージョンに関わらず動作すること。

・管理画面、エージェントともにマイクロソフトWindows11以降のOSへの対応は、適時報告を行うこと。

4.3.既存ネットワーク環境及びクライアント端末の管理ツールへの対応

既存ネットワーク、次期ネットワークの環境下（16.3「ネットワーク構成」参照)で動作可能であること。

4.4.構築期間・コストの最小化

本システムの構築にあたっては、要求する機能を実現しながら、可能な限り構築期間及びコストを最小化できるような手法を採用すること。

4.5.ソフトウェアに関する知識

本業務に従事する者は、セキュリティ対策の業務について一定程度の知識と経験を有し、本システムの構築・運用について提案が出来ること。

5.業務内容

システム納入完了までの業務内容は概ね以下のとおりである。

業務	内容(詳細作業)
1プロジェクト管理業務	・業務計画の作成（体制を含む） ・進捗、工程管理作業(スケジュールの遅延が発生しそうな場合の事前対策の策定、実施等も含む) ・課題管理作業 ・その他関連作業
2設計業務	・要件定義 ・フィット＆ギャップ分析 ・カスタマイズ設計 ・その他関連作業
3構築業務	・ハードウェアの設定作業(ハードウェアの新規導入が必要な場合) ・ソフトウェアのインストール作業、設定作業 ・教育研究所ネットワークへの接続作業 ・初期データの取り込み、設定作業 ・その他関連作業（教育研究所指示書記載の作業含む）
4運用準備業務	・各種テスト作業（教育研究所の確認作業含む） ・その他関連作業
5研修業務	・システム管理者への研修作業（研修用ドキュメント作成含む） ・システムユーザーへの研修作業（研修用ドキュメント作成含む）

6.納入物

本業務の納入物は概ね以下のとおりである。それぞれの様式及び納期については、契約締結時の協議により定める。

納入物	内容
1システム本体	本システムの環境構築を行い利用可能な状態で納入をおこなうもの ・本システム一式(OS、DB、ミドルウェア等のパッケージを含む)
2ドキュメント類	本システムの環境構築に伴い作成した各種ドキュメント(紙及び電子媒体) ・プロジェクト管理関連一式(プロジェクト管理資料 等) ・設計関連一式(要件定義書 等) ・構築関連一式(構築作業手順書、設定シート 等) ・テスト関連一式(テスト計画書、テスト結果報告書 等) ・研修関連一式(研修マニュアル、研修実施報告書 等) ・マニュアル類(システム管理者用マニュアル、システム操作マニュアル) ・その他(研究所との打ち合わせ議事録 等)

7.スケジュール概要

本システム運用開始までのスケジュール概要は以下を想定している。

各パッケージ製品等に照らし、契約締結後7日以内にスケジュール概要と業務計画を提示すること。その際、下表のスケジュールを前倒し可能であれば検討するものとする。

※詳細スケジュールは、教育研究所との協議の上決定する

項目	7月	8月	9月
キックオフ			
導入打ち合わせ			
サーバー設定			
端末にインストール			
管理開始			
各種ドキュメント納付			

8.クライアント端末へのインストール手順

端末へのエージェントのインストール手順は次のように想定している。
インストーラーでの入力項目は必要最小限にし、簡単にインストールできるようにすること
各パッケージ製品等に照らし、修正・具体化した作業工程を提案時に提示すること。

(1)クラウドサービスにおける管理サーバー稼働

(2)対象小学校のインストーラー作成

(3)対象学校の端末に資産管理ツール（SKYSEA）を用いてインストーラー配付、実行してもらう

(4)管理画面から得られるインストール済クライアント端末データとPC管理簿のデータを照合

(5)インストールできないクライアント端末があれば教育研究所で調査後、導入業者が行う

9.システム機能要件

9.1.機能概要

本システムは、後述の「EDR機能要件一覧」に示す機能を有するものとする。

10.規模要件

10.1.管理対象ハードウェア

・令和6年度端末入れ替え対象校（城北小学校・泊小学校・識名小学校・壺屋小学校・与儀小学校・城岳小学校・古蔵小学校・大名小学校）端末約500台　(OS:Windows10,Windows11)

10.2.ユーザー数

本システムは、少なくとも以下のユーザーが利用することを想定している。
・部門管理担当者 約15名（教育研究所　情報支援G職員）
・対象校教職員等 約300名

11.性能要件

本システムの利用時には、ネットワーク遅延等の場合を除き、画面表示がもたつくことなく、ストレスの無い画面遷移や応答速度を確保すること。
また、一定規模の同時アクセスに対応でき、排他制御についても適切に行われること。
※「サービスレベル」で提示を求めるサービスレベルに内容を記載すること。

12.情報セキュリティ要件

12.1.権限設定

本システムでは、権限のない者による各種情報へのアクセスやデータの改ざんが行なわれないように、適切なアクセス権限の設定ができること。

12.2.情報セキュリティ対策

本システムについて「那覇市学校教育情報セキュリティポリシー」を確実に遵守すること。
特に以下の対策は確実に実施すること。
(1)セキュリティパッチ
・システム側のサーバーに搭載するOSのセキュリティ脆弱性に関する情報に注意し、最新のセキュリティパッチが適用できるよう運用設計すること。
・セキュリティパッチを適用することにより、自身並びに他のソフトウェアが動作不良をおこさないよう、事前の検討または検証をおこなうこと。
・エージェントを搭載するクライアント端末のOS（マイクロソフトWindowsシリーズ）のセキュリティ脆弱性に関する情報に注意し、最新のセキュリティパッチが適用できるよう運用設計すること。
・エージェント側のセキュリティパッチを適用することにより、自身並びに他のソフトウェアが動作不良をおこさないよう、事前の検討または検証をおこなうこと。

(2)セキュリティ対策ソフト
・システム側のサーバーにはファイアウォール、IDS、IPS、アンチウイルスソフトウェアなどのセキュリティソフトウェアを適用すること、クラウドタイプならばプロバイダーによるセキュリティ対策が整っていることを確認すること。
・運用時は最新のパターンファイルを適用し、定期的なスキャンとあわせて確認管理を実施できること。
・ネットワーク接続には、VPNなどの暗号化技術を使用すること。
・エージェントがインストールされるクライアント端末のセキュリティ対策ソフトセキュリティの設定と相性の問題を起こさないこと。

13.拡張性等要件

13.1.拡張性要件

将来の管理対象クライアント端末数及びユーザー数の増分に対応できること、その際のライセンス料も提示すること。

13.2.上位互換性要件

管理対象クライアント端末 OS のバージョンアップ等に対応できること。特に、クライアント端末のOSが Windowsの次期バージョンへの対応は、適時報告を行うこと。

13.3.システム中立性要件

本システムについては、本資料に特に断りがない限り、極力、標準的な技術を用いること。ハードウェアの新規導入が必要な場合は、メーカーを特定せず調達・運用ができるよう留意すること。

14.運用要件

14.1.システム稼働・監視等要件

・システムの運用時間は、原則として 24 時間 365 日とする。
・システムを停止させる必要がある場合には、あらかじめ研究所に連絡する等の調整を行うこと。また、想定されるシステム停止の頻度について示すこと。
・障害の発生を未然に防止又は速やかに発見できる機能を有すること。

14.2.データ管理要件

・本システムで扱うすべてのデータの保全が実施できる環境であること。
・データの消失を防ぐため、定期的にバックアップをおこなう機能を有すること。
・バックアップしたデータを速やかにリストアできる機能を有すること。

14.3.運用施設・設備要件

本システムで使用する電源量は省電力構成を図ること。

15.保守要件

保守要件は、以下のとおりとし、運用を円滑におこなうための保守対応(操作方法や仕様に関する問い合わせを含む)について、本提案内で提示すること。

15.1.保守体制

・保守対応時間は、土曜、日曜、祝日及び年末年始(12月29日から1月3日)及び6月23日（慰霊の日）を除く、平日の9時から17時とする。ただし、緊急を要する場合の対応については、契約時に研究所と協議の上、決定するものとする。
・サービスが停止するハードウェアのメンテナンス等は、教育研究所と連絡と協議をおこない、年末年始(12月29日から1月3日)、春・夏・秋休み、ゴールデンウィーク等の休日もしくはユーザーの業務時間外に行うこと。
・サービスが停止しないメンテナンス等は、教育研究所と連絡と協議をおこない処理日と時間を決定すること。
・研究所からの情報伝達方法は、電話及びメールとし、それらを受ける環境を整備すること。また、受け付けた旨を必ず2営業日以内に返答するものとし、対応が長期にわたるものについては、適時進捗を連絡するものとする。
・点検、障害復旧等の対応が完了したものについては、報告書(故障箇所、内容、対処策など)を作成し、すみやかに研究所に提出すること。
・本システムに故障が発生しないように予防措置に関する情報提供を適宜おこなうこと。

15.2.ソフトウェア保守

・システムの機能的な不具合(いわゆるバグ等)やセキュリティの脆弱性の修正は、その規模に関わらず、追加費用の発生しない基本保守の範囲内とする。
・運用に重大な支障を及ぼす不具合、及びシステムの停止を伴う障害については、迅速に対応し、最短時間で復旧させること。ただし、復旧までの進捗状況については適宜報告を行うこと。
・本システムを構成するソフトウェアについて、セキュリティホール及びバージョンアップ情報等が公開された場合、速やかに研究所へ報告し対応をおこなうこと。
・本システムの運用開始後に、ベースとなったシステムに機能追加があった場合は、その内容について適宜通知すること。
・上記、追加機能の本システムへの実装については、基本保守契約で対応可能な範囲を提示の上、必要に応じて拡張保守契約の提案をおこなうこと。

15.3.ハードウェア保守

・本提案において、ハードウェアの新規調達をおこなわない場合においても、故障箇所がハードウェアかソフトウェアか特定する切り分け作業は、基本保守の範囲内とする。
・ハードウェアの新規導入をおこなう場合についての保守要件は以下のとおりとするが、ハードウェア故障に係る保守費用についても、入札価格に含めて応札すること。
(1)故障箇所がハードウェアであった時には、現状の機器もしくは同等以上の能力を有する機器(部品交換含む)を用意し、速やかに復旧対応すること。
(2)本システムを構成するハードウェアのファームウェアに対して、セキュリティホール及びバージョンアップ情報等が公開された場合、速やかに研究所へ報告し対応すること。

16.システム稼働環境

16.1.ハードウェア構成

・本件システムのサーバーはクラウドでの運用とする。
・クラウドサービス提供者の推奨スペックを参考に、必要なCPU数・メモリ・ストレージ容量等を考慮して応札すること。
・クラウドサービス提供者の推奨スペックを参考に、適切な規模のインスタンスとストレージ設定を提案すること。
・~~両者共に、~~停電、落雷等におけるシステム障害を回避するため安全にシャットダウンできる無停電電源装置を備えた構成であること。
・~~両者共に、グリーン購入法に基づく機器の調達をおこなうこと。~~

16.2.ソフトウェア構成

・本システムの性質及び利用規模等を考慮し、サーバーを構成するOS、DB、およびその他のミドルウェア等を適切に選定すること。
・選定したOS、DB、およびその他のミドルウェア等の調達費用を構築費用に含めること。
・管理対象クライアント端末へは、エージェント以外のソフトウェア(ActiveXコントロールなどのプラグインを含む)をインストールすることなく利用できる構成とすること。
・その他ソフトウェアの具体的な実装については特に定めないが、標準的なものを利用すること。

16.3.ネットワーク構成

本システムが接続されるネットワークの概要は以下のとおりである。
【現状】
・校務系と学習系（GIGAネットワーク）に2系統で運用されており、教諭用パソコンは両方のネットワークに接続して仕事することが可能。
（1）校務系　小・中学校、出先機関⇔本庁⇔データセンター⇔インターネットでセンター集約型の形でネットに接続される各拠点間のの接続速度は100mbps、1Gbps、1Gbps（ベストエフォート）・100mbpsの専用線　　※小・中学校54校、出先機関4箇所
（2）学習系　各小・中学校からローカルブレイクアウト形式でインターネットに接続されている。
接続速度は1Gbps（ベストエフォート）
【将来】
・校務系は学習系に統合予定で、フルクラウドに移行予定です。

・EDRを稼働するに当たってネットワークのポート設定変更等を要する場合は、保守業者による変更料金も含めて応札するものとする。

17.テスト要件

・本システムの本格運用に必要なテストを行い、都度、教育研究所の承認を受けること。
・研究所が指定する期日までに、テスト結果を記したテスト結果報告書を作成し、提出すること。
・テストの実施方法、実施内容、実施時期などを提案すること。

18.教育

・システム運用のためのマニュアルを、システム管理者に提供すること。
　マニュアルは電子データで提供すること。
・システム管理者に対する、運用及び操作研修を実施すること（オンライン可）。
・研修の実施方法、内容、実施時期について提案すること。

19.システム構築時の作業体制及び方法

19.1.体制・役割

(1)体制
　本業務を統括し、研究所との窓口となる責任者を設置すること。
特に定めない限り、責任者等との連絡は教育研究所の通常業務時間内(平日の8:30~17:15)は電話対応できるものとし、教育研究所との協議により必要と判断した場合は教育研究所への派遣をおこなうものとする。
(2)担当者
　業務の実施体制には、類似のシステムの構築経験を有する者を含むこと。
(3)報告・協議等
　システム構築の各段階において、進捗状況や問題点等を教育研究所へ報告、協議するものとし、その頻度等については契約締結時に協議し確定するものとする。

19.2.管理方法

・プロジェクトの管理には、PMBOKに基づく一般的なプロジェクトマネジメントの知識と慣行を適用すること。
・教育研究所が指定する期日までにプロジェクト管理基準を記したプロジェクト計画書及び関連資料を作成し、提出すること。なお、作業実施体制図と作業スケジュールは、本提案内にて提示すること。

19.3.導入・引き渡しに関する要件

　本システムについて、設置、ハードウェアの調整、サーバー側ソフトウェアのインストール、データのセッティング等の関係する環境構築を行い、利用可能な状態で納入をおこなうものとする。

20.サービスレベル

　本システムの性能、信頼性、運用、保守等に係るサービスレベルを設定し、サービスレベルの測定方法も含めて、本提案内にて提示することとし、その内容については、契約締結時に協議し確定するものとする。

21.ウィルス対策ソフトおよびEDR機能要件

(1) Windows 10,11に導入可能であること
(2) Windows Server 2016,2019,2022に導入可能であること
(3) Redhat Linux、CentOSに導入可能であること
(4) MacOSに導入可能であること
(5) 単一エージェントでエンドポイント防御機能を提供できること
(6) リアルタイム検索機能を有すること
(7) 予約検索機能を有すること
(8) オンデマンド検索機能を有すること
(9) 既知マルウェアを検出・ブロックできる機能を有すること
(10) AMSI(Microsoft Antimalware Scan Interface) を利用した防御機能を有すること
(11) ファイルレスマルウェアに対応した防御機能を有すること
(12) ディープラーニングを利用した検出・ブロックできる機能を有すること
(13) ランサムウェア攻撃を検知し、ロールバックできる機能を有すること
(14) ランサムウェアにより暗号化されたファイルを復旧させる際にボリュームシャドウコピーを利用せずに復元できること
(15) マスターブートレコードを暗号化するランサムウェア攻撃を検知・ブロックできる機能を有すること
(16) リモートからのランサムウェア攻撃に対する防御機能を有すること
(17) ブラウザに存在する脆弱性を攻撃して Web ブラウザに感染する MITB (Man-in-the-Browser) 攻撃を防止する機能を有すること
(18) ブラウザの Cookie を保護する機能を有すること
(19) マルウェア検知時にプロセスの停止やファイルのクリーンアップ機能を有すること
(20) 脅威を駆除した後に脅威の侵入経路およびファイルに対する影響範囲（発生日時、アプリケーションなど）などをマッピングして表示する機能を有すること
(21) デバイスへの攻撃と思われる検知が確認された場合に、Safeモードの再起動を防止するなどといった形で保護レベルが自動的に高くなる機能を有すること
(22) Safeモードで起動しても保護機能を保持し続けること
(23) URLフィルタリング機能を有すること
(24) Webサイトを評価するURLレピュテーションを有すること
(25) ダウンロードしたファイルを評価するレピュテーション機能を有すること
(26) USBメモリやMTP/PTP接続デバイスといった、外部機器の接続に対して制御する機能を有すること
(27) アプリケーションコントロール機能を有すること
(28) 情報漏えい対策（DLP）機能を有すること
(29) EDRで検知した内容を管理コンソールで確認できること
(30) エンドポイント製品以外のアラートを同一画面で確認することができること
(31) アラートごとに通知することなく、一連のアラートを自動的にまとめる機能を有すること
(32) 収集したデータを管理コンソールから調査できるツールを有すること
(33) 脅威インテリジェンスを利用したアラートの重要度を自動判別し可視化できること
(34) クラウド上のデータだけでなく、エンドポイント端末に対してもクエリ検索できること
(35) 他社製品のアラートを取り込む機能を有すること
(36) 管理コンソールから端末やサーバーに接続し、プロセスの停止やファイルの削除などができる機能を有すること

21.1管理要件

(1) 社内に管理サーバーを用意することなく、クラウドサービスで提供されること
(2) データセンターの指定を日本含め複数国からできること
(3) 管理コンソールの言語表示は日本語に対応していること
(4) システムチューニングの必要があるならば、業者側で設定・対応すること
(5) アクセスログファイルの改ざん、削除を防御する機能を有すること
(6) 管理者以外がアンインストールできないような機能を有すること

21.2展開要件

(1) 同一インストーラで複数の端末やサーバーに導入することが可能であること
(2) ~~ActiveDirectoryまたは、~~資産管理ツール（SKYSEA）を利用したエージェントの展開が可能であること
(3) 管理画面で端末ごとにEDR機能を開始できること
(4) アンインストールできる実行ファイルを有すること、もしくは管理画面で端末のEDR機能を停止できること
(5) 非インターネット接続端末やサーバーに導入できる仕組みを有すること
(6) 非インターネット接続端末やサーバーに導入している実績があること

21.3保守要件

(1) ベンダーが有するサポートセンターを利用することができること
(2) サポートが日本語対応できること
(3) 新任担当職員へのコントロール操作の説明・レクチャーを少なくとも年１回実施すること

21.4その他の要件

(1) MDRに更新できる機能を有すること
(2) 1ライセンスから追加購入できること
(3) ライセンス追加した場合の、契約終了月は任意に選択できること
(4) 国内で導入実績があること
(5) 契約期間は複数年契約とし、月払いとすること